

P14683-A



日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日  
Date of Application:

2001年 1月12日

出願番号  
Application Number:

特願2001-005002

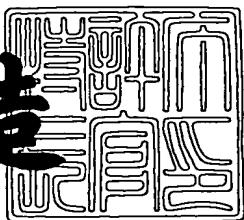
出 願 人  
Applicant(s):

## 日本電信電話株式会社

2001年 6月13日

特許庁長官  
Commissioner,  
Japan Patent Office

# 及川耕造



出証番号 出証特2001-3055434

【書類名】 特許願  
【整理番号】 NTTI126778  
【提出日】 平成13年 1月12日  
【あて先】 特許庁長官殿  
【国際特許分類】 G06K 9/00  
【発明者】  
【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内  
【氏名】 重松 智志  
【発明者】  
【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内  
【氏名】 森村 浩季  
【発明者】  
【住所又は居所】 東京都千代田区大手町二丁目3番1号 日本電信電話株式会社内  
【氏名】 町田 克之  
【特許出願人】  
【識別番号】 000004226  
【氏名又は名称】 日本電信電話株式会社  
【代理人】  
【識別番号】 100064621  
【弁理士】  
【氏名又は名称】 山川 政樹  
【電話番号】 03-3580-0961  
【手数料の表示】  
【予納台帳番号】 006194  
【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701512

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証トークンおよび認証システム

【特許請求の範囲】

【請求項1】 通常時はユーザにより所持されるとともに、そのユーザの認証データに応じて所定の処理を行う利用機器をユーザが利用する場合には、その利用機器へ接続されて前記ユーザの生体情報に基づきユーザ認証を行う認証トークンであって、

前記ユーザの生体情報を検出し、その検出結果をセンシングデータとして出力するセンサと、

前記ユーザの生体情報を照合するための登録データが予め格納されている記憶回路と、

前記記憶回路に記憶されている登録データを用いて前記センサからのセンシングデータを照合し、ユーザ認証結果を示すその照合結果を認証データとして出力する照合回路と、

この照合回路からの認証データを通信データとして前記利用機器へ送信する通信回路とが、一体に形成されていることを特徴とする認証トークン。

【請求項2】 請求項1記載の認証トークンにおいて、

前記記憶回路は、前記利用機器での処理に用いられる前記ユーザに固有のユーザ情報を予め記憶し、

前記照合回路は、前記記憶回路から読み出した前記ユーザ情報を前記認証データに含めて出力することを特徴とする認証トークン。

【請求項3】 請求項1または2記載の認証トークンにおいて、

前記通信回路からの通信データを所定のデータ形式へ変換して前記利用機器へ送信するプロトコル変換回路をさらに備えることを特徴とする認証トークン。

【請求項4】 請求項1または2記載の認証トークンにおいて、

前記通信回路からの通信データを無線区間を介して前記利用機器へ送信する無線回路をさらに備えることを特徴とする認証トークン。

【請求項5】 請求項3記載の認証トークンにおいて、

前記プロトコル変換回路からの通信データを無線区間を介して前記利用機器へ

送信する無線回路をさらに備えることを特徴とする認証トークン。

【請求項6】 請求項1～5記載の認証トークンにおいて、

当該認証トークン内へ電源供給を行う電池をさらに備えることを特徴とする認証トークン。

【請求項7】 請求項6記載の認証トークンにおいて、

前記電池は、当該認証トークンが前記利用機器へ接続された際にその利用機器からの電源供給により充電される二次電池からなることを特徴とする認証トークン。

【請求項8】 所定の処理を行う利用機器を利用する場合に必要なユーザ認証をユーザの生体情報を用いて行う認証システムであって、

通常時はユーザにより所持されるとともに、ユーザが前記利用機器を利用する場合はその利用機器へ接続されて前記ユーザの生体情報に基づきユーザ認証を行う認証トークンを備え、

前記認証トークンは、前記ユーザの生体情報を検出しその検出結果をセンシングデータとして出力するセンサと、前記ユーザの生体情報を照合するための登録データが予め格納されている記憶回路と、前記記憶回路に記憶されている登録データを用いて前記センサからのセンシングデータを照合し、ユーザ認証結果を示すその照合結果を認証データとして出力する照合回路と、この照合回路からの認証データを通信データとして前記利用機器へ送信する第1の通信回路とを有するとともに、これら回路部が一体として形成されており、

前記利用機器は、前記認証トークンから送信された通信データを受信し認証データとして出力する第2の通信回路と、この第2の通信回路からの認証データに含まれる照合結果に基づき前記所定の処理を行う処理回路とを備えることを特徴とする認証システム。

【請求項9】 請求項8記載の認証システムにおいて、

前記認証トークンの記憶回路は、前記利用機器での処理に用いられる前記ユーザに固有のユーザ情報を予め記憶し、

前記認証トークンの照合回路は、前記記憶回路から読み出した前記ユーザ情報を前記認証データに含めて出力し、

前記利用機器の処理回路は、前記第2の通信回路からの認証データに含まれるユーザ情報を用いて処理を行うことを特徴とする認証システム。

【請求項10】 請求項8または9記載の認証システムにおいて、

前記認証トークンに接続され、前記認証トークンの前記第1の通信回路からの通信データを所定のデータ形式へ変換して前記利用機器へ送信するデータ変換モジュールをさらに備えることを特徴とする認証システム。

【請求項11】 請求項8または9記載の認証システムにおいて、

前記認証トークンに接続され、前記認証トークンの前記第1の通信回路からの通信データを無線区間を介して前記利用機器へ送信する無線モジュールをさらに備え、

前記利用機器は、前記無線モジュールから送信された前記通信データを無線区間を介して受信し前記第2の通信回路へ出力する無線回路を有することを特徴とする認証システム。

【請求項12】 請求項10記載の認証システムにおいて、

前記認証トークンに接続され、前記データ変換モジュールからの通信データを無線区間を介して前記利用機器へ送信する無線モジュールをさらに備え、

前記利用機器は、前記無線モジュールから送信された前記通信データを無線区間を介して受信し前記第2の通信回路へ出力する無線回路を有することを特徴とする認証システム。

【請求項13】 請求項8または9記載の認証システムにおいて、

前記認証トークンは、当該認証トークン内へ電源供給を行う電池をさらに有することを特徴とする認証システム。

【請求項14】 請求項10または12記載の認証システムにおいて、

前記データ変換モジュールは、当該データ変換モジュール内および前記認証トークンへ電源供給を行う電池をさらに有することを特徴とする認証システム。

【請求項15】 請求項11または12記載の認証システムにおいて、

前記無線モジュールは、当該無線モジュール内および前記認証トークンへ電源供給を行う電池をさらに有することを特徴とする認証システム。

【請求項16】 請求項13～15記載の認証システムにおいて、

前記電池は、前記認証トークンが前記利用機器へ接続された際にその利用機器からの電源供給により充電される二次電池からなることを特徴とする認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、認証トークンおよび認証システムに関し、特に人間の生体情報を用いてユーザ本人であることを認証するための認証トークンおよび認識システムに関するものである。

【0002】

【従来の技術】

高度情報化社会では、情報処理との親和性を持って厳密にユーザ本人を認証したいという要求が高い。特に、予め承認したユーザだけに入室を許可する入室管理システムや個人情報などの重要な情報を扱うような情報管理システム、あるいは電子決済を行う決済システムなどでは、上記のような要求が極めて高い。

このような要求に対し、半導体装置の製造技術や情報処理技術をベースとして、電子的に検出した固有の生体情報に基づきユーザ本人を認証するための認証システムの研究が盛んに行われている。

【0003】

従来、このような認証システムは、図4に示すような構成となっていた。図4に従来の認証システムのブロック図を示す。

この認証システムでは、例えばユーザ認証が得られた場合に処理装置84で所定のサービスを提供する利用機器8内に、センサ81、記憶回路82および照合回路83が設けられている。センサ81では指紋などの生体情報を電子的に検出し、得られたセンシングデータ81Aを照合回路83へ出力する。一方、記憶回路82にはユーザの生体情報を照合するための情報が登録指紋データ82Aとして記憶されている。

【0004】

照合回路83では、記憶回路82から読み出した登録指紋データ82Aを用い

てセンサ81からのセンシングデータ81Aを照合することにより、ユーザ認証を行う。そして、その認証結果を認証データ83Aとして処理装置84へ出力する。処理装置84では、照合回路83からの認証データ83Aが認証成功を示す場合にのみ、所定のサービスをユーザに対して提供する。

また、図5に示すように、記憶回路82のみを所持可能なデータカード9へ分離したものも考えられる。この場合には、サービス提供時、個々のユーザが所持するデータカード9が利用機器8へ接続され、利用機器8内に設けられた通信回路85を介して、記憶回路82に記憶されている登録指紋データ82Aが登録指紋データ85Aとして照合回路83へ読み込まれて照合される。

#### 【0005】

##### 【発明が解決しようとする課題】

しかしながら、このような従来の認証システムでは、ユーザの生体情報を検出するセンサ81や照合を行う照合回路83を利用機器8内部に設け、ユーザの生体情報を照合するための情報すなわち登録指紋データ82Aを用いて照合を行うものとなっているため、次のような問題点があった。

まず、前者（図4参照）によれば、①利用機器8内部の記憶回路82にユーザの登録指紋データ82Aが予め登録されていないと、ユーザはたとえ本人であってもサービスを受けることは不可能である。また、②サービスを提供する全機器に多数ユーザの登録指紋データを記憶させるには、その配信方法や記憶方法が複雑かつ大規模になり、そのためコストの増加や安全性の低下を招いてしまう。さらに、③機器に自分の指紋データが登録されているのは、ユーザのプライバシー問題も引き起こし、心理的にも受け入れがたいシステムになってしまふ。

#### 【0006】

これに対し、後者（図5参照）の認証システムでは、ユーザの登録データをデータカード9でユーザ自身が所持し管理するため、上記①～③の問題は回避できるが、④照合時にはユーザの登録指紋データがサービス機器に送信されるため、そのデータ漏洩に対する対策が必要であり、システムの規模が大きくなってしまう。さらに、⑤生体情報を検出するセンサ81が不特定多数のユーザ間で共有しているため、センサ81の故障時にはその機器に対するサービスが全て利用でき

なくなってしまう。また、⑥指紋などのようにセンサに対して人体の一部を接触させる必要がある場合は、センサ81の共用によりユーザに対する衛生面でも問題があり、これらを解決するためにはシステムの規模が増大してしまう。

本発明はこのような課題を解決するためのものであり、照合時に用いる登録データの漏洩を防止でき、またセンサ故障による影響を最小限にとどめ、さらにはユーザに対して良好な衛生環境を保つことができる認証システムを提供することを目的としている。

#### 【0007】

##### 【課題を解決するための手段】

このような目的を達成するために、本発明にかかる認証トークンは、通常時はユーザにより所持されるとともに、そのユーザの認証データに応じて所定の処理を行う利用機器をユーザが利用する場合には、その利用機器へ接続されてユーザの生体情報に基づきユーザ認証を行う認証トークンであって、ユーザの生体情報を検出しその検出結果をセンシングデータとして出力するセンサと、ユーザの生体情報を照合するための登録データが予め格納されている記憶回路と、記憶回路に記憶されている登録データを用いてセンサからのセンシングデータを照合し、ユーザ認証結果を示すその照合結果を認証データとして出力する照合回路と、この照合回路からの認証データを通信データとして利用機器へ送信する通信回路とを一体に形成したものである。

#### 【0008】

この場合、認証トークンの記憶回路で、利用機器での処理に用いられるユーザに固有のユーザ情報を予め記憶しておき、照合回路で、記憶回路から読み出したユーザ情報を認証データに含めて出力するようにしてもよい。

また、データ形式が異なる各種利用機器に対応するため、認証トークンの第1の通信回路からの通信データを所定のデータ形式へ変換して利用機器へ送信するプロトコル変換回路を設けてもよい。さらに、利用機器と無線区間を介して接続するため、認証トークンの第1の通信回路からの通信データあるいはプロトコル変換回路からの通信データを無線区間を介して利用機器へ送信する無線回路を設けてもよい。

また、認証トークン内に電池を設け、当該認証トークン内へ、具体的にはセンサ、記憶回路、照合回路および通信回路へ、さらにはプロトコル変換回路や無線回路へ電源供給を行うようにしてもよい。この電池として二次電池を用い、当該認証トークンが利用機器へ接続された際にその利用機器からの電源供給により充電するようにしてもよい。

#### 【0009】

また、本発明にかかる認証システムは、所定の処理を行う利用機器を利用する場合に必要なユーザ認証をユーザの生体情報を用いて行う認証システムであって、通常時はユーザにより所持されるとともに、ユーザが利用機器を利用する場合はその利用機器へ接続されてユーザの生体情報に基づきユーザ認証を行う認証トークンを備え、認証トークンに、ユーザの生体情報を検出しその検出結果をセンシングデータとして出力するセンサと、ユーザの生体情報を照合するための登録データが予め格納されている記憶回路と、記憶回路に記憶されている登録データを用いてセンサからのセンシングデータを照合し、ユーザ認証結果を示すその照合結果を認証データとして出力する照合回路と、この照合回路からの認証データを通信データとして利用機器へ送信する第1の通信回路とを設けてこれら回路部を一体として形成し、利用機器に、認証トークンから送信された通信データを受信し認証データとして出力する第2の通信回路と、この第2の通信回路からの認証データに含まれる照合結果に基づき所定の処理を行う処理回路とを設けたものである。

#### 【0010】

この場合、認証トークンの記憶回路で、利用機器での処理に用いられるユーザに固有のユーザ情報を予め記憶しておき、照合回路で、記憶回路から読み出したユーザ情報を認証データに含めて出力し、利用機器の処理回路で、第2の通信回路からの認証データに含まれるユーザ情報を用いて処理を行うようにしてもよい。

また、データ形式が異なる各種利用機器に対応するため、認証トークンの第1の通信回路からの通信データを所定のデータ形式へ変換して利用機器へ送信するデータ変換モジュールを認証トークンに接続して用いるようにしてもよい。さら

に、利用機器と無線区間を介して接続するため、認証トークンの第1の通信回路からの通信データを無線区間を介して利用機器へ送信する無線モジュールを認証トークンに接続して用い、また利用機器に、無線モジュールから送信された通信データあるいはデータ変換モジュールからの通信データを無線区間を介して受信し第2の通信回路へ出力する無線回路を設けるようにしてもよい。

#### 【0011】

また、認証トークンに電池を設け、その電池から認証トークン内へ電源供給を行うようにしてもよく、さらにデータ変換モジュールや無線モジュールへも電源供給するようにしてもよい。また、データ変換モジュールや無線モジュールに電池を設け、当該モジュールおよび認証トークンへ電源供給を行うようにしてもよい。

また、これら電池として二次電池を用い、当該認証トークンが利用機器へ接続された際にその利用機器からの電源供給により充電するようにしてもよい。

#### 【0012】

##### 【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して説明する。

図1は本発明の第1の実施の形態にかかる認証トークンおよびその認証トークンを用いた認証システムを示すブロック図である。

この認証システムは、ユーザ認証が得られた場合にサービスを提供する利用機器2と、通常時はユーザに所持されサービス提供時に利用機器2へ接続されてユーザの生体情報を用いたユーザ認証を行う認証トークン1とから構成されている。なお、本発明において、トークンとは、ユーザが所持し持ち運び可能な小型軽量の装置を指し、認証トークンとは、ユーザ本人の認証を行う機能を持つトークンをいう。以下では、生体情報として指紋を用いる場合を例として説明するが、生体情報としては、このほか声紋、虹彩、筆跡、手のひら形状（指の関節長）、静脈パターン、顔面配置パターンなどを用いることも可能である。

#### 【0013】

認証トークン1には、指紋（生体情報）を読み取るセンサ11、ユーザ本人の登録指紋データ12Aやユーザ情報12Bを記憶する記憶回路12、センサ11

での読み取り結果を示すセンシングデータ11Aを、記憶回路12に記憶されている登録指紋データ12Aを用いて照合する照合回路13、この照合回路13での照合結果を含む認証データ13Aを通信データ1Aとして認証トークン1の外部へ送信する通信回路14が設けられており、これら回路部を一体として形成する認証トークン1が利用機器2に対して着脱自在に接続される。

利用機器2には、認証トークン1からの通信データ1Aを受信する通信回路21と、受信した通信データ1Aに含まれる照合結果が一致を示す場合にのみ、そのユーザへのサービス提供を行う処理装置22とが設けられている。

#### 【0014】

次に、図1を参照して、本実施の形態の動作について説明する。

ユーザは事前に、自分の所持する認証トークン1の記憶回路12に、自分の登録指紋データ12Aやサービスを利用するためのパスワードや個人情報などからなるユーザ情報12Bを記憶させておく。

利用機器2を利用する際、まずユーザは自分の認証トークン1を利用機器2へ接続し、指をそのセンサ11へ置く。これにより認証トークン1のセンサ11でユーザの指紋が読み取られセンシングデータ11Aとして出力される。このセンシングデータ11Aは照合回路13において記憶回路12の登録指紋データ12Aを用いて照合される。そして、その照合結果を含む認証データ13Aが出力される。このとき照合回路13は、記憶回路12に予め記憶回路12に格納されているユーザID、パスワード、個人情報などのユーザ情報12Bを読み出し、認証データ13Aへ含めて出力する。

#### 【0015】

通信回路14では、照合回路13からの認証データ13Aを通信データ1Aとして利用機器2へ送信する。

利用機器2の通信回路21では、認証トークン1の通信回路14から送信された通信データ1Aを受信し、認証データ13と同じ内容の認証データ21Aとして出力する。処理装置22では、この認証データ21Aを受け取ってその認証データ21Aに含まれる照合結果を参照する。そして、その照合結果が一致を示す場合、処理装置22においてユーザの所望する所定の処理が実行される。

## 【0016】

このように、本実施の形態では、ユーザの指紋を検出しその検出結果をセンシングデータとして出力するセンサ11と、ユーザの指紋を照合するための登録指紋データ12Aが予め格納されている記憶回路12と、この記憶回路12に記憶されている登録指紋データ12Aを用いてセンサ11からのセンシングデータ11Aを照合し、ユーザ認証結果となるその照合結果を認証データとして出力する照合回路13と、この照合回路13からの認証データを通信データ1Aとして利用機器2へ送信する通信回路14とを、認証トークン1として一体として形成したものである。

## 【0017】

そして、認証に応じて所定の処理を行う利用機器2をユーザが利用する場合には、認証トークン1をその利用機器2へ接続し、その認証トークン1でユーザの生体情報に基づきユーザ認証を行い、利用機器2へ通知するようにしたものである。

また、利用機器2に、認証トークン1から送信された通信データ1Aを受信し認証データ21Aとして出力する通信回路21と、この通信回路21からの認証データ21Aに含まれる照合結果に基づき所定の処理を行う処理装置22とを設け、この利用機器2とは独立した各ユーザが個々の持つ認証トークン1での認証結果に基づき所定の処理を行うようにしたものである。

## 【0018】

したがって、従来のように、ユーザの生体情報を検出するセンサや照合を行う照合回路を利用機器内部に設け、ユーザの登録データをデータカードでユーザ自身が所持し管理する場合と比較して、登録データが認証トークンの外部へ出力されなくなることにより照合時に用いる登録データの漏洩を防止できる。また、センサを不特定多数のユーザで共用する必要がなく、ユーザが個々に所持する認証トークンごとに設けられているセンサを用いるため、センサ故障が発生しても他のユーザには波及せず、さらに生体情報検出の際、指紋などのようにセンサに対して人体の一部を接触させる必要がある場合でもユーザに対して良好な衛生環境を保つことができる。

## 【0019】

認証トークン1については、ユーザが所持するのに適するように、上記のセンサ、記憶回路および照合回路などの各種回路が一体に形成、すなわち同一の筐体に収容されている。この場合、これらの各種回路を同一基板上に形成してもよく、これらの各種回路を1チップの半導体装置として形成する技術（例えば、特開2000-242771号公報など参照）を用いることで、非常に小型な認証トークンを実現することも可能となる。

## 【0020】

さらに、記憶回路12にユーザIDやパスワードさらには個人情報などのユーザ情報12Bを予め記憶しておき、これらを認証データ13Aに含めて利用機器2へ送信するようにしたので、利用機器2の処理装置22において、その認証データに含まれるユーザ情報12B、例えばユーザIDやパスワードをチェックすることにより処理実行の可否を判断でき、利用機器で行う処理の重要性に合わせた基準で認証判定できる。また、ユーザ情報12Bの個人情報、例えば氏名、住所、電話番号、口座番号やクレジットカード番号などを処理に用いることにより、処理に必要な個人情報をユーザが入力する必要がなくなり、ユーザの操作負担を大幅に軽減できる。

## 【0021】

次に、図2を参照して、第2の実施の形態について説明する。図2は本発明の第2の実施の形態にかかる認証システムを示すブロック図である。本実施の形態は、上記第1の実施の形態の認証システム（図2参照）のうち、認証トークン1の出力段にデータ変換モジュール3を付加したものである。

このデータ変換モジュール3には、認証トークン1の通信回路14から出力された通信データを、利用機器2で受信・解読可能なデータ形式へ変換するプロトコル変換回路31が設けられている。

## 【0022】

このように、認証トークン1に着脱自在に取り付けられるデータ変換モジュール3を介して、所望の利用機器2と認証トークン1とを接続するようにしたので、データ形式が異なる利用機器に対しても同一認証トークンを用いたユーザ認証

が可能となる。また、様々な形式に対応したデータ変換モジュールを用意し、それらを認証トークンに対して容易に着脱交換することで、ユーザが1つの認証トークンを用いて様々な利用機器を利用することができ、複数の認証トークンを所持する必要がない。また、1つのデータ変換モジュールを複数のユーザで共用することも可能である。

以上では、データ変換モジュール3を認証トークン1に対して着脱自在に取り付ける場合を例として説明したが、認証トークン1内部にプロトコル変換回路31を設けてもよく、さらにコンパクトに構成できる。

#### 【0023】

次に、図3を参照して、第3の実施の形態について説明する。図3は本発明の第3の実施の形態にかかる認証システムを示すブロック図である。本実施の形態は、上記第1の実施の形態の認証システム（図1参照）のうち、認証トークン1の出力段に無線モジュール4を付加したものである。

この無線モジュール4には、認証トークン1の通信回路14から出力された通信データを、利用機器2で受信・解読可能なデータ形式へ変換するプロトコル変換装置41と、このプロトコル変換装置41からの通信データを無線区間を介して利用機器2へ送信する無線回路42とが設けられている。この場合、利用機器2側にも無線回路23を設ける必要がある。

#### 【0024】

このように、認証トークン1に着脱自在に取り付けられる無線モジュール4を用いて、所望の利用機器2と認証トークン1とを接続するようにしたので、ユーザは、認証トークン1を利用機器2に直接接続することなく、例えば自分の手元で認証トークン1を用いてユーザ認証を行いサービスを受けることが可能となる。したがって、利用機器2に対して認証トークン1を接続する作業や、利用機器2に接続されている状態の認証トークン1を用いて認証を行う作業など、認証時のユーザに対する作業負担を大幅に軽減できる。

#### 【0025】

また、様々な通信プロトコルに対応した無線モジュールを用意し、それらを認証トークンに対して容易に着脱交換することで、ユーザが1つの認証トークンを

用いて様々な利用機器を利用することができるようになる。さらに、1つの無線モジュールを複数のユーザで共用することも可能である。

なお、利用機器2と認証トークン1の通信プロトコルが同一の場合は、無線モジュール4のプロトコル変換回路41を省略することも可能である。また、無線回路42の代わりに、赤外線通信回路や超音波通信回路など、無線区間を介してデータ通信可能な通信回路を用いてもよい。

以上では、無線モジュール4を認証トークン1に対して着脱自在に取り付ける場合を例として説明したが、認証トークン1内部に無線回路42やプロトコル変換回路41を設けてもよく、さらにコンパクトに構成できる。また、認証トークン1と利用機器2との間でやり取りする認証データや通信データに対して暗号化方式を用いてもよく、上記各実施の形態について適用できる。

#### 【0026】

以上で説明した第1～第3の実施の形態において、認証トークン1やデータ変換モジュール3、無線モジュール4への電力は、認証トークン内に設けた電池を用いて供給するようにしてもよい。また、認証トークン1が利用機器2に接続されている状態で、利用機器2内の電源から認証トークン1へ電源供給するようにしてもよい。このとき、認証トークン1内の電池として充電可能な二次電池を用い、利用機器2と接続状態にあるときに、利用機器2内の電源を用いてその二次電池を充電するようにしてもよい。

また、非接触カードなどで用いられる非接触電力供給技術を用いて、利用機器から認証トークン1やデータ変換モジュール3、無線モジュール4への電源供給や、二次電池の充電を行うようにしてもよい。

なお、認証トークン1に対する電力供給については、上記構成例に限定されるものではない。

#### 【0027】

以上で説明した第2の実施の形態において、データ変換モジュール3内に設けた電池を用いて、データ変換モジュール3や認証トークン1の各回路へ電力供給するようにしてもよい。また、このデータ変換モジュール3内の電池として充電可能な二次電池を用い、利用機器2の電源を用いてこの二次電池を充電するよう

にしてもよい。

以上で説明した第3の実施の形態において、無線モジュール4内に設けた電池を用いて、無線モジュール4や認証トークン1の各回路へ電源供給するようにしてもよい。また、この無線モジュール4内の電池として充電可能な二次電池を用い、利用機器2の電源を用いてこの二次電池を充電するようにしてもよい。

#### 【0028】

##### 【発明の効果】

以上説明したように、本発明は、ユーザの生体情報を検出し、その検出結果をセンシングデータとして出力するセンサと、ユーザの生体情報を照合するための登録データが予め格納されている記憶回路と、記憶回路に記憶されている登録データを用いてセンサからのセンシングデータを照合し、ユーザ認証結果を示す。その照合結果を認証データとして出力する照合回路と、この照合回路からの認証データを通信データとして利用機器へ送信する通信回路とを、認証トークンとして一体に形成し、この認証トークンを通常時はユーザにより所持し、ユーザが利用機器を利用する場合はその利用機器へ接続してユーザの生体情報に基づきユーザ認証を行うようにしたものである。

#### 【0029】

したがって、従来のように、ユーザの生体情報を検出するセンサや照合を行う照合回路を利用機器内部に設け、ユーザの登録データをデータカードでユーザ自身が所持し管理する場合と比較して、登録データが認証トークンの外部へ出力されることはなくなり、照合時に用いる登録データの漏洩を防止できる。また、センサが不特定多数のユーザで共用されず、ユーザが個々に所持する認証トークンごとに設けられているため、センサ故障が発生しても他のユーザには波及せず、さらに生体情報を検出する際に指紋などのようにセンサに対して人体の一部を接触させる必要がある場合でもユーザに対して良好な衛生環境を保つことができる。

##### 【図面の簡単な説明】

【図1】 本発明の第1の実施の形態による認証トークンおよび認証システムを示すブロック図である。

【図2】 本発明の第2の実施の形態による認証トークンおよび認証システ

ムを示すブロック図である。

【図3】 本発明の第3の実施の形態による認証トークンおよび認証システムを示すブロック図である。

【図4】 従来の認証システムを示すブロック図である。

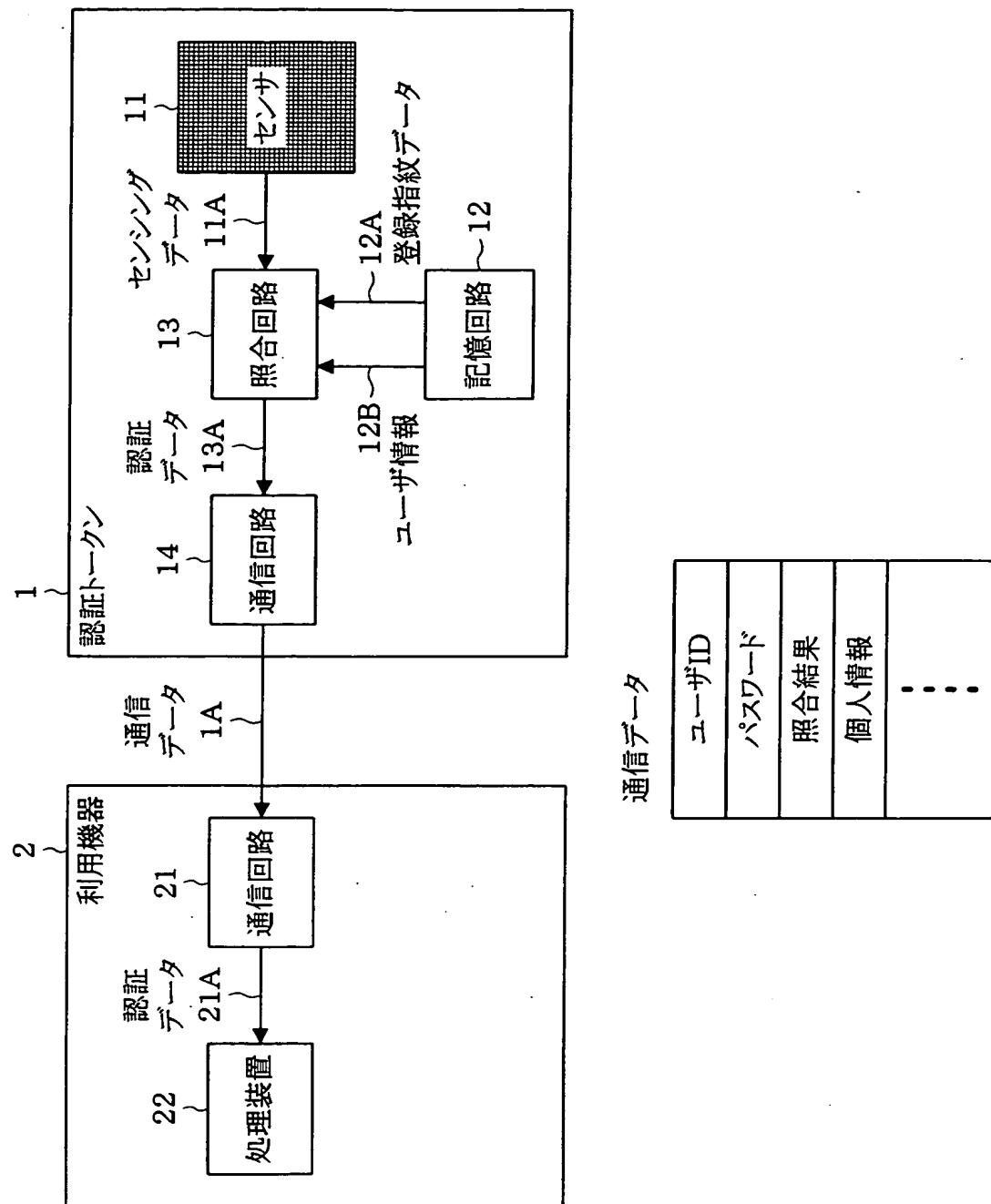
【図5】 従来の他の認証システムを示すブロック図である。

【符号の説明】

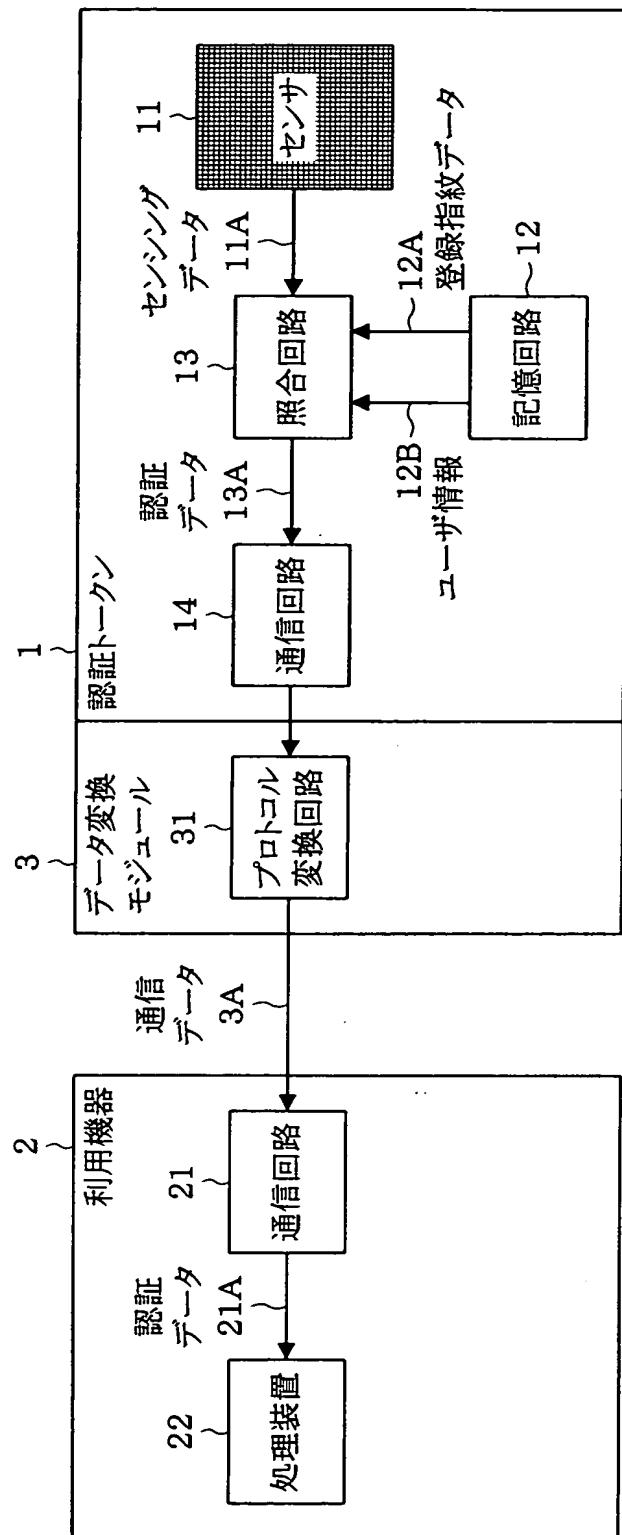
1 …認証トークン、 1 1 …センサ、 1 2 …記憶回路、 1 2 A …登録指紋データ  
、 1 2 B …ユーザ情報、 1 3 …照合回路、 1 3 A …認証データ、 1 4 …通信回路  
、 1 A …通信データ、 2 …利用機器、 2 1 …通信回路、 2 1 A …認証データ、 2  
2 …処理装置、 2 3 …無線回路、 3 …データ変換モジュール、 3 1 …プロトコル  
変換回路、 3 A …通信データ、 4 …無線モジュール、 4 1 …プロトコル変換回路  
、 4 2 …無線回線、 4 A …通信データ。

【書類名】図面

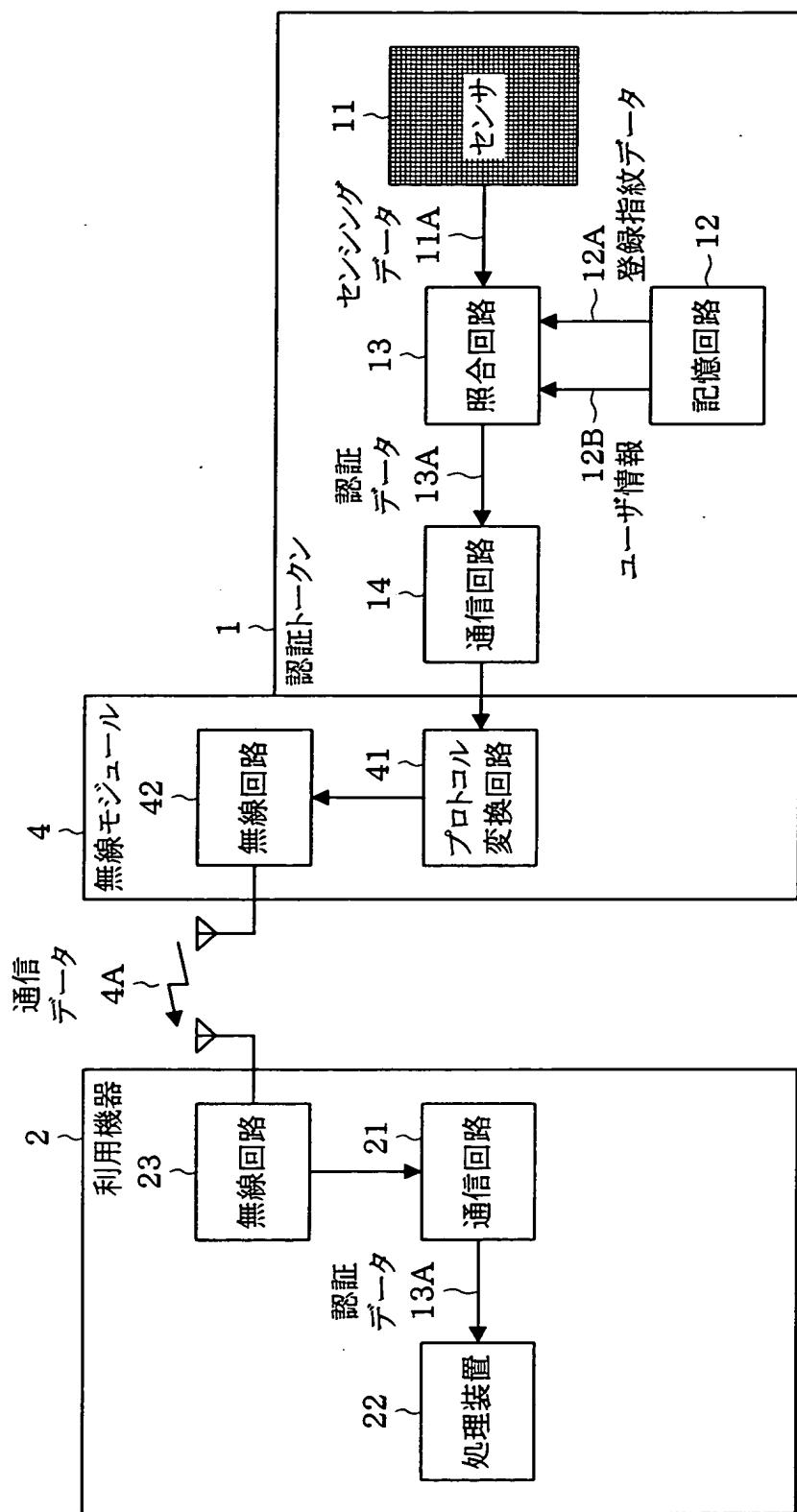
【図1】



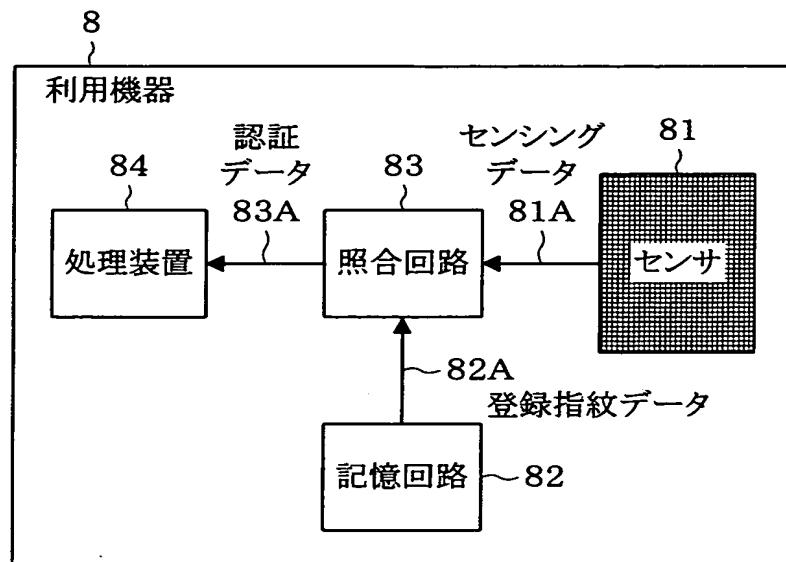
## 【図2】



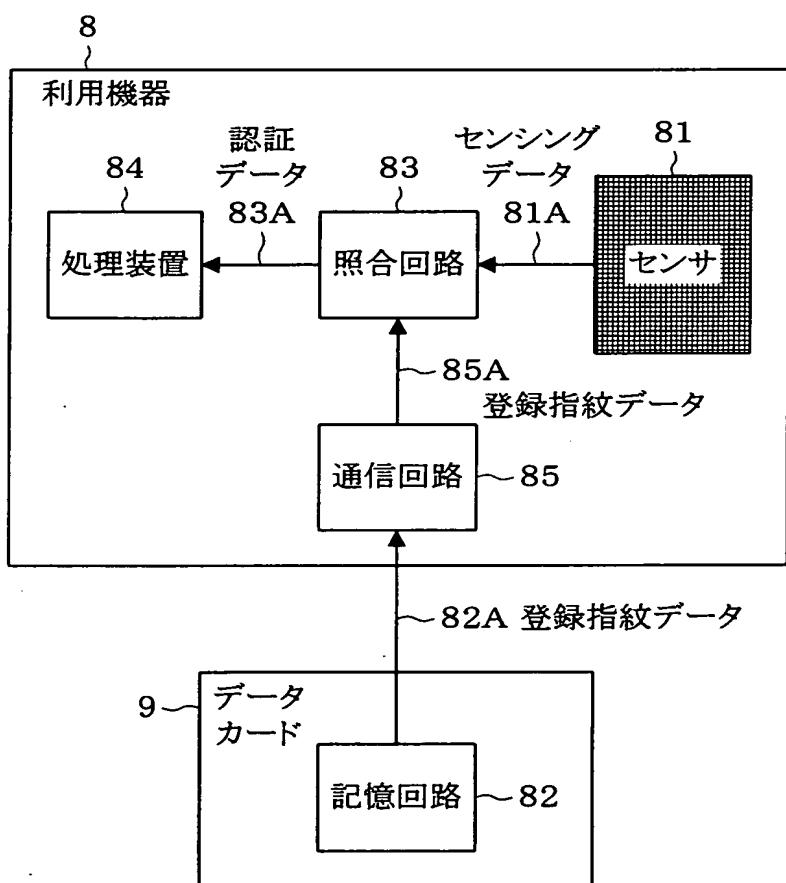
【図3】



【図4】



【図5】



【書類名】 要約書

【要約】

【課題】 照合時に用いる登録データの漏洩を防止でき、またセンサ故障による影響を最小限にとどめ、ユーザに対して良好な衛生環境を保つようとする。

【解決手段】 認証トークン1では、センサ11、記憶回路12、照合回路13および通信回路14を一体として形成し、センサ11によりユーザの指紋を検出し、その検出結果をセンシングデータ11Aとして出力する。照合回路13では、記憶回路12に記憶されている登録指紋データ12Aを用いてセンサ11からのセンシングデータ11Aを照合し、ユーザ認証結果を示す。その照合結果を認証データとして出力し、この認証データを通信回路14から通信データ1Aとして前記利用機器2へ送信する。利用機器では、認証トークン1から通信データ1Aとして受信した認証データに基づき所定の処理を実行する。

【選択図】 図1

出願人履歴情報

識別番号 [000004226]

1. 変更年月日 1999年 7月15日

[変更理由] 住所変更

住 所 東京都千代田区大手町二丁目3番1号

氏 名 日本電信電話株式会社